

# **Energy Provider Community of Interest**

## **Build Team and Energy Provider Community Meeting**

**29 June 2016**

## **Securing Networked Infrastructure for the Energy Sector**

## Agenda

- NCCoE news
- Current projects
  - Identity and Access Management (IdAM) project update
  - Situational Awareness (SA) project update
- SA Build Team introduction and overview
- Open discussion

## NCCoE Out and About:

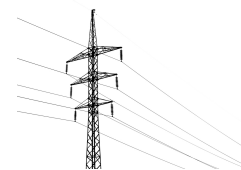
- Attended conferences
  - Webinar with AlertEnterprise (June) – *Jim McCarthy*
  - Cybersecurity for Oil & Gas Summit (June) – *Jim McCarthy*
- Upcoming planned conferences
  - EnergySec (August)
  - Power Grid Cyber Security Exchange (August)
  - ICS Cyber Security Conference Sacramento (October)
  - GridSecCon (October) – *potential workshop*
  - World Congress on Industrial Control Systems Security (WCICSS) (December)

## Identity and Access Management (IdAM) Project

- Provides a reference solution to:
  - Authenticate individuals and systems
  - Enforce authorization control policies
  - Unify IdAM services
  - Protect generation, transmission and distribution
  - Improve awareness and management of visitor accesses
  - Simplify the reporting process
- Draft guide is online at [https://nccoe.nist.gov/projects/use\\_cases/idam](https://nccoe.nist.gov/projects/use_cases/idam)
- *Final Guide publication pending final approvals*
- Demonstrations and adoption support available

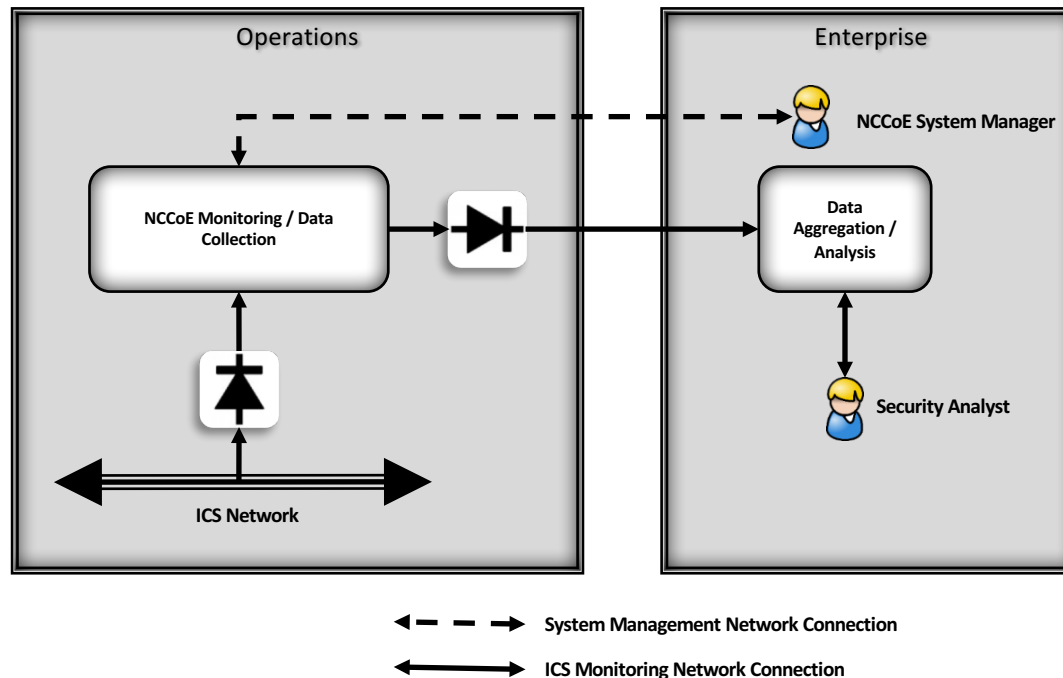


Converged  
management of silos



## Situational Awareness Project









- Improve OT availability
- Detect anomalous conditions and remediation; unify visibility across silos
- Investigate events leading to baseline deviations/ anomalies and share findings
- Use Case published:  
[http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE\\_ES\\_Situational\\_Awareness.pdf](http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf)









PROJECT NAME: IdAM	Upcoming Milestone Dates
Publish Special Publication	Thu 06/30/16

PROJECT NAME: Situational Awareness	Upcoming Milestone Dates
Completed Build	Wed 07/13/16
Release Draft Practice Guide for Public Comments	Thu 08/25/16
Publish Special Publication	Thu 11/24/16

# SITUATIONAL AWARENESS BUILD TEAM INTRODUCTION

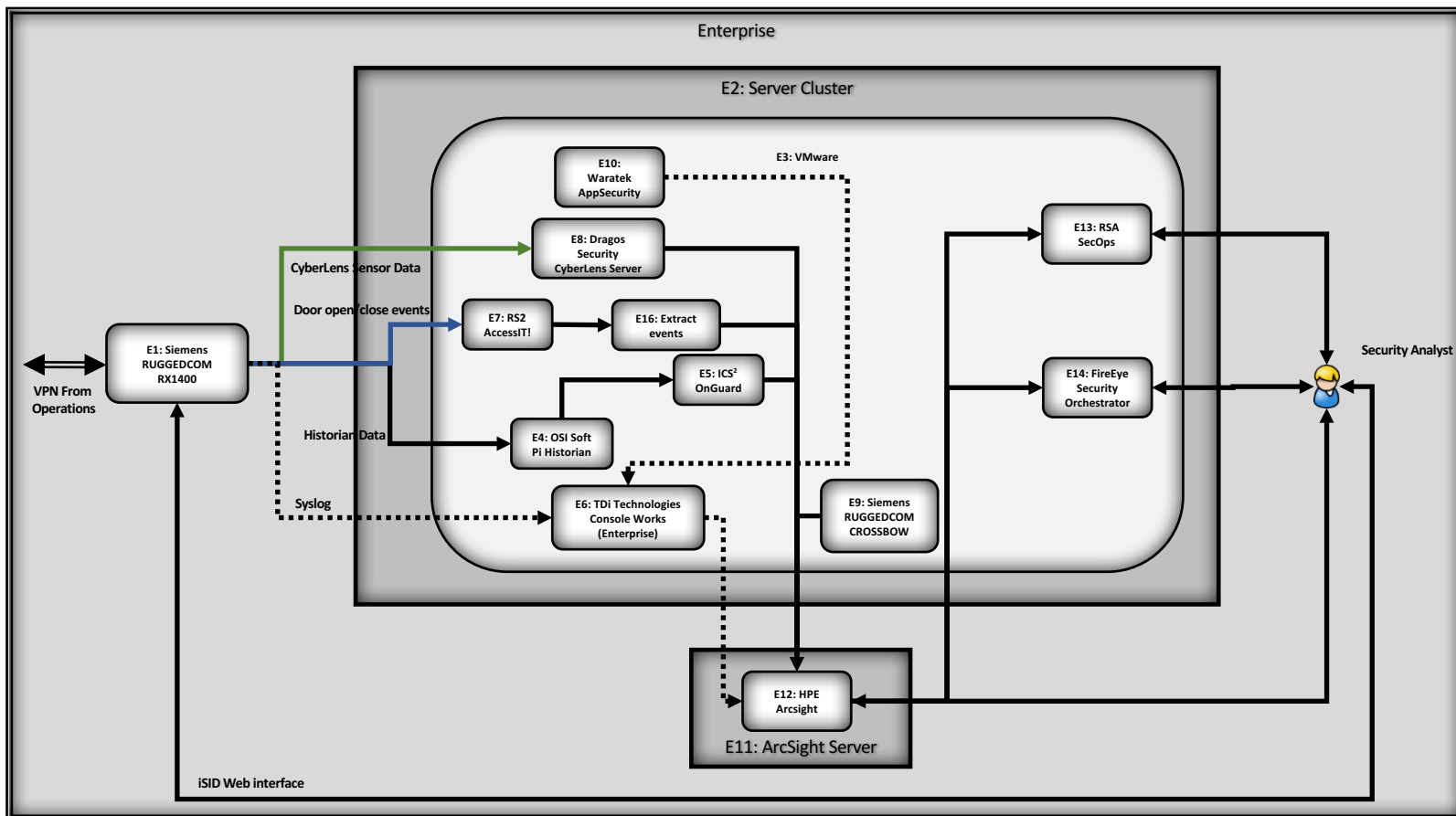
Company	Logo	POC	Product links	Application to SA project build
Dragos Security		Rob Lee, <a href="mailto:rob@dragossecurity.com">rob@dragossecurity.com</a> Jon Lavender, <a href="mailto:jon@dragossecurity.com">jon@dragossecurity.com</a>	<a href="https://www.dragossecurity.com/products/cyberlens">https://www.dragossecurity.com/products/cyberlens</a>	ICS Asset management
HPE ArcSight		Bruce Oehler, <a href="mailto:bruce.oehler@hpe.com">bruce.oehler@hpe.com</a> Steve Roberts, <a href="mailto:Steve.roberts4@hpe.com">Steve.roberts4@hpe.com</a>	<a href="http://www.hpe.com">http://www.hpe.com</a>	Security information and event management (SIEM) platform
ICS2		Anis Bishara, <a href="mailto:anisb@ics2.com">anisb@ics2.com</a>		Operational Behavior Anomaly Detection
FireEye Invotas		Paul Nguyen, <a href="mailto:paul.nguyen@FireEye.com">paul.nguyen@FireEye.com</a>	<a href="https://www.fireeye.com/products/security-orchestrator.html">https://www.fireeye.com/products/security-orchestrator.html</a>	Security orchestrator/incident remediation playbook
OSIsoft		Paul Geraci, <a href="mailto:pgeraci@osisoft.com">pgeraci@osisoft.com</a>	<a href="http://www.osisoft.com">http://www.osisoft.com</a>	PI system
PPC		Matt McDonald, <a href="mailto:matt.mcdonald@ppc.com">matt.mcdonald@ppc.com</a> Steve J. Sage, <a href="mailto:ssage@ppc.com">ssage@ppc.com</a>		PI system
Radiflow		Ayal Vogel, <a href="mailto:ayal_v@radiflow.com">ayal_v@radiflow.com</a> , Dario Lobo, <a href="mailto:Dario_L@radiflow.com">Dario_L@radiflow.com</a>	OT Security Brochure - <a href="http://radiflow.com/downloads/OT%20Security/Security%20OT%20Brochure.pdf">http://radiflow.com/downloads/OT%20Security/Security%20OT%20Brochure.pdf</a> Security Gateway Data Sheet - <a href="http://radiflow.com/3180-secure-ruggedized-router/">http://radiflow.com/3180-secure-ruggedized-router/</a> SCADA Intrusion Detection Data-Sheet - <a href="http://radiflow.com/products/isid-intrusion-detection-system/">http://radiflow.com/products/isid-intrusion-detection-system/</a>	SCADA Intrusion detection/Deep Packet SCADA Firewall
RSA		Ben Smith, <a href="mailto:ben.smith@rsa.com">ben.smith@rsa.com</a>	<a href="https://www.rsa.com/en-us/products-services/security-operations/security-operations-management-secps">https://www.rsa.com/en-us/products-services/security-operations/security-operations-management-secps</a>	Security operations dashboard

# SITUATIONAL AWARENESS BUILD TEAM INTRODUCTION (2)

Company	Logo	POC	Product links	Application to SA project build
RS2 Technologies		Dave Barnard, <a href="mailto:dbarnard@RS2tech.com">dbarnard@RS2tech.com</a>	<a href="http://www.rs2tech.com">www.rs2tech.com</a>	Physical access control system
Schneider Electric		Mike Pyle, <a href="mailto:michael.pyle@schneider-electric.com">michael.pyle@schneider-electric.com</a>		Industrial control system firewall
Siemens		Jeff Foley, <a href="mailto:jeff.foley@siemens.com">jeff.foley@siemens.com</a>  AJ Nicolosi, <a href="mailto:aj.nicolosi@siemens.com">aj.nicolosi@siemens.com</a>	<u>RX1500</u> <a href="http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/switches-routers-layer-3/Pages/rx1500.aspx">http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/switches-routers-layer-3/Pages/rx1500.aspx</a> <u>RX1400</u> <a href="http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/switches-routers-layer-3/Pages/rx1400.aspx">http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/switches-routers-layer-3/Pages/rx1400.aspx</a> <u>CROSSBOW</u> <a href="http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/software/Pages/crossbow.aspx">http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/software/Pages/crossbow.aspx</a>	Industrial control system remote management authentication platform/ configuration management
TDi Technologies		Bill Johnson, <a href="mailto:bill.johnson@tditechnologies.com">bill.johnson@tditechnologies.com</a>	<a href="http://www.tditechnologies.com/">http://www.tditechnologies.com/</a> <a href="http://www.tditechnologies.com/products/nerc-cip-smart-grid-solutions">http://www.tditechnologies.com/products/nerc-cip-smart-grid-solutions</a> <a href="http://www.tditechnologies.com/our-customers/utilities">http://www.tditechnologies.com/our-customers/utilities</a>	Industrial control system and infrastructure remote management (IT / OT)
Waratek		Nollaig Heffernan, <a href="mailto:nheffernan@waratek.com">nheffernan@waratek.com</a>		SQL injection prevention
Waterfall Security		Andrew Ginter, <a href="mailto:Andrew.ginter@waterfall-security.com">Andrew.ginter@waterfall-security.com</a>	<a href="http://waterfall-security.com/products/unidirectional-security-gateways">http://waterfall-security.com/products/unidirectional-security-gateways</a> <a href="http://waterfall-security.com/products/secure-bypass">http://waterfall-security.com/products/secure-bypass</a>	Unidirectional gateway



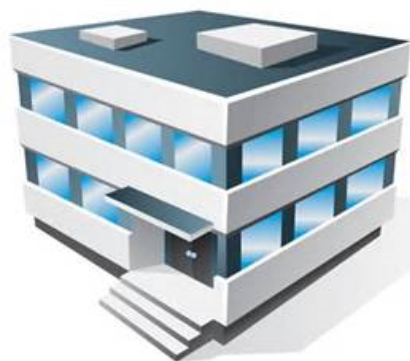




Updated June 27, 2016



301-975-0200

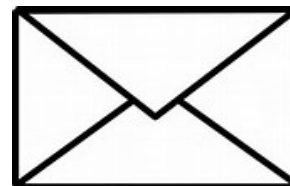


9700 Great Seneca Hwy,  
Rockville, MD 20850

<http://nccoe.nist.gov/forums/energy>



[energy\\_nccoe@nist.gov](mailto:energy_nccoe@nist.gov)



100 Bureau Drive, Mail Stop 2002,  
Gaithersburg, MD 20899

*Thank You*

# ABOUT THE NCCOE

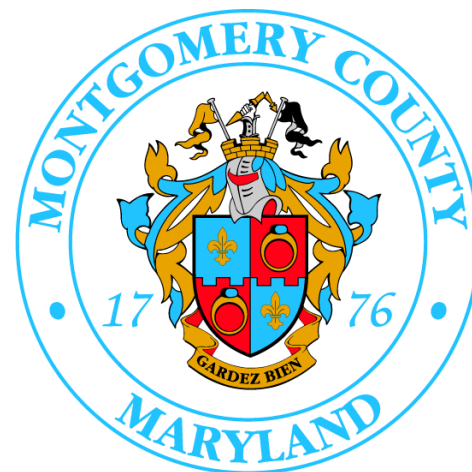




## Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®

Department of Business & Economic Development





## VISION

### ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

## MISSION

### ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs



## GOAL 1

### PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

## GOAL 2

### INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

## GOAL 3

### ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

## The NCCoE seeks problems that are:

- ▶ Broadly applicable across much of a sector, or across sectors
- ▶ Addressable through one or more reference designs built in our labs
- ▶ Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

## Reference designs address:

- ▶ Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- ▶ Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)



## Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards



## Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications



## Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions



## Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry



## Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



## Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results



